REMARKS

After entry of the foregoing amendment, claims 26-70 are pending in the application.

The Section 112 issue has been addressed by removing the term "computations" in claim 47. A similar change has been made in claims 62 and 70.

Concerning audio signals, essentially all of the references to audio in the priority specifications concern *steganographically* encoding a signal in such audio.

The Field of the Invention paragraph in the 1993 priority specification noted:

> *The present invention relates to the field of identifying signals and images as to origin and ownership. Specifically, it relates to the need in the commercial* ***audio*** *and visual industry* ***to unequivocally identify a multi-generation copy of source material based on objective methods*** *rather than purely subjectively and perceptually based opinion.*

The techniques disclosed in this specification for "unequivocally identifying a multi-generational copy of source material based on objective methods" rest on steganographic encoding.

That specification goes on to note:

> *What is needed is a much simpler and truly cost effective method for performing a positive identification between a copy of an original signal and the original. This method should not only be able to perform positive identification, it should also be able to relate version identification of sold copies in order to better pinpoint the point of sale. The method should not compromise the innate quality of material which is being sold, as does the placement of localized logos on images. The method should be robust so that an identification can be made even after multiple copies have been made and/or compression and decompression of the signal has taken place. The identification method should be largely uneraseable or "uncrackable." The method should be capable of working even on fractional pieces of the original signal, such as a 10 second "riff" of an* ***audio*** *signal or the "clipped and pasted" sub-section of an original image.*
>
> *The existence of such a method would have profound consequences on* ***audio*** *and image piracy in that it could A) cost effectively monitor for unauthorized uses of material and perform "quick checks"; B) become a deterrent to unauthorized uses when the method is known to be in use and the consequences well publicized; and C) provide unequivocal proof of identity, similar to fingerprint identification, in litigation, with potentially more reliability than that of fingerprinting.*
>
> ...

> *In accordance with a preferred embodiment of the invention, a computer systems is provided with associated means for manipulating either digital* ***audio*** *signals or digital images. In cases where original material is in "non-digital" form, such as on* ***audio*** *tape or on a photograph, means for creating a high fidelity digital copy of the material is included in the preferred embodiment. This physical system will be referred to as the "Eye-D" workstation or system which serves as a concise trade name. The Eye-D system* ***embeds an imperceptible global signal*** *either directly onto the digital original or onto the "digitized copy" of the original if it was in a non-digital form to begin with. The new copy with the embedded signal becomes the material which is sold while the original is secured in a safe place. The new copy will be nearly identical to the original except under the finest of scrutiny; thus, its commercial value will not be compromised. After the new copy has been sold and distributed and potentially distorted by multiple copies, the present disclosure details a method for positively identifying any suspect signal against the original.*

The embedding of an imperceptible signal is steganographic encoding of a signal.[1]

A variety of other excerpts might be cited, but the foregoing are believed to establish the requisite support.

Claim 26 stands rejected over Moses (5,404,377) in view of Schwab (5,134,496). Claim 50 stands rejected over O'Grady (4,969,041) in view of Gniewek (5,265,082). Applicant respectfully traverses these rejections. For example, the Action wrongly characterizes Schwab as teaching use of imperceptibly embedded signals to prevent copying. However, Schwab is understood to teach an arrangement in which "code sequences are visually manifested as dropouts on a video monitor" (Abstract) and as a "video imperfection" (col. 2, line 26). This is not "imperceptible" (even if, to some viewers, it may be "acceptable"). No reference to imperceptibility is found in Schwab.

[1] Steganography is the art/science of hiding one information signal in another carrier. Two references are enclosed to illustrate this meaning.

One is Kawaguchi, "Principles and Applications of BPCS-Steganography," Proc. Of SPIE, Vol. 3528, pp. 464-73, Nov 2-4, 1998, which states at page 1 "Steganography is a technique to hide secret information in some other data (we call it a vessel) without leaving any apparent evidence of data alteration."

The other is WO 02/13436, which states at page 1, ""Data hiding or steganography is the art of hiding a message signal in a host signal, without any perceptual distortion of the host signal... Though steganography is often confused with the relatively well-known cryptography, the two are but loosely related. Cryptography is about hiding the contents of a message. Steganography, on the other hand, is about concealing the very fact that a message is hidden. Steganography may be considered as communication through subliminal channels, or secret communications."

Likewise, the analysis of claim 50 is believed to be flawed. The Examiner tries to equate the claimed "plural sequential series of audio data" to plural frames of video in O'Grady. However, applicant's claim requires processing "a plurality of series of said encoded audio signal" with the processing unit to extract the auxiliary data. O'Grady, in contrast, doesn't work this way. His elements 68/70 are understood to operate on less than a single frame (i.e., the data period T referenced at column 3, line 43 is said to be 7050 samples – less than a frame, as indicated at column 5, line 37). Thus, the parallel perceived by the Examiner (i.e., decoding extending across plural frames) is not understood to be present.

Since the Action has not established a *prima facie* case under § 103, further comments on the rejections (e.g., the alleged teachings of Gniewek, and the proposed combination) are not belabored.

No rejection was made as to claims 51-64; these are understood to have been objected-to for the dependence on rejected claim 50, but should now likewise be in condition for allowance.

In view of the foregoing, the application is believed to be in condition for allowance, and action to that end is solicited.

Respectfully submitted,

Date: June 8, 2004

CUSTOMER NUMBER 23735

DIGIMARC CORPORATION

Phone: 503-885-9699
FAX 503-885-9880

By____________________________
William Y. Conwell
Registration No. 31,943

Principle and applications of BPCS-Steganography

Eiji Kawaguchi* and Richard O. Eason**

* Kyushu Institute of Technology, Kitakyushu, Japan
** University of Maine, Orono, Maine 04469-5708

ABSTRACT

Steganography is a technique to hide secret information in some other data (we call it a vessel) without leaving any apparent evidence of data alteration. All of the traditional steganographic techniques have limited information-hiding capacity. They can hide only 10% (or less) of the data amounts of the vessel. This is because the principle of those techniques was either to replace a special part of the frequency components of the vessel image, or to replace all the least significant bits of a multi-valued image with the secret information.

Our new steganography uses an image as the vessel data, and we embed secret information in the bit-planes of the vessel. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. We can replace all of the "noise-like" regions in the bit-planes of the vessel image with secret data without deteriorating the image quality. We termed our steganography "BPCS-Steganography," which stands for Bit-Plane Complexity Segmentation Steganography.

We made an experimental system to investigate this technique in depth. The merits of BPCS-Steganography found by the experiments are as follows.

1. The information hiding capacity of a true color image is around 50%.
2. A sharpening operation on the dummy image increases the embedding capacity quite a bit.
3. Canonical Gray coded bit planes are more suitable for BPCS-Steganography than the standard binary bit planes.
4. Randomization of the secret data by a compression operation makes the embedded data more intangible.
5. Customization of a BPCS-Steganography program for each user is easy. It further protects against eavesdropping on the embedded information.

Keywords: steganography, data hiding, information hiding, BPCS, digital picture envelope, vessel image, dummy image, encryption, compression, bit plane

1. INTRODUCTION

Internet communication has become an integral part of the infrastructure of today's world. The information communicated comes in numerous forms and is used in many applications. In a large number of these applications, it is desired that the communication be done in secrete. Such secret communication ranges from the obvious cases of bank transfers, corporate communications, and credit card purchases, on down to a large percentage of everyday email. With email, many people wrongly assume that their communication is safe because it is just a small piece of an enormous amount of data being sent worldwide. After all, who is going to see it? But in reality, the Internet is not a secure medium, and there are programs "out there" which just sit and watch messages go by for interesting information.

Encryption provides an obvious approach to information security, and encryption programs are readily available. However, encryption clearly marks a message as containing "interesting" information, and the encrypted message becomes subject to attack. Furthermore, in many cases it is desirable to send information without anyone even noticing that information has been sent.

Steganography presents another approach to information security. In steganography, data is hidden inside a vessel or container that looks like it contains only something else. A variety of vessels are possible, such as digital images, sound clips, and even executable files. In recent years, several steganographic programs have been posted on Internet home pages. Most

Part of the SPIE Conference on Multimedia Systems and Applications
Boston, Massachusetts • November 1998
SPIE Vol. 3528 • 0277-786X/98/$10.00

of them use image data for the container of the secret information. Some of them use the least significant bits of the image data to hide the data. Other programs embed the secret information in a specific band of the spatial frequency component of the carrier. Some other programs make use of the sampling error in image digitization. However, all those steganographic techniques are limited in terms of information hiding capacity. They can embed only 5-15 % of the vessel image at the best. Therefore, current steganography is more oriented to water marking of computer data than to secret person-person communication applications.

We have invented a new technique to hide secret information in a color image. This is not based on a programming technique, but is based on the property of human vision system. Its information hiding capacity can be as large as 50% of the original image data. This could open new applications for steganography leading to a more secure Internet communication age.

Digital images are categorized as either binary (black-and-white) or multi-valued pictures despite their actual color. We can decompose an n-bit image into a set of n binary images by bit-slicing operations [1][2]. Therefore, binary image analysis is essential to all digital image processing. Bit slicing is not necessarily the best in the Pure-Binary Coding system (PBC), but in some cases the Canonical Gray Coding system (CGC) is much better [3].

2. THE COMPLEXITY OF BINARY IMAGES

The method of steganography outlined in this paper makes use of the more complex regions of an image to embed data. There is no standard definition of image complexity. Kawaguchi discussed this problem in connection with the image thresholding problem, and proposed three types of complexity measures [4][5][6]. In the present paper we adopted a black-and-white border image complexity.

The definition of image complexity

The length of the black-and-white border in a binary image is a good measure for image complexity. If the border is long, the image is complex, otherwise it is simple. The total length of the black-and-white border equals to the summation of the number of color-changes along the rows and columns in an image. For example, a single black pixel surrounded by white background pixels has the boarder length of 4.

We will define the image complexity α by the following.

$$\alpha = \frac{k}{\text{The max. possible B - W changes in the image}} \qquad (1)$$

Where, k is the total length of black-and-white border in the image. So, the value ranges over

$$0 \leq \alpha \leq 1. \qquad (2)$$

(1) is defined globally, i.e., α is calculated over the whole image area. It gives us the global complexity of a binary image. However, we can also use α for a local image complexity (e.g., an 8 × 8 pixel-size area). We will use such α as our local complexity measure in this paper.

3. ANALYSIS OF INFORMATIVE AND NOISE-LIKE REGIONS

Informative images are simple, while noise-like images are complex. However, this is only true in cases where such binary images are part of a natural image. In this section we will discuss how many image patterns are informative and how many patterns are noise-like. We will begin by introducing a "conjugation" operation of a binary image.

1. Conjugation of a binary image

Let P be a $2^N \times 2^N$ size black-and-white image with black as the foreground area and white as the background area. W and B denote all-white and all-black patterns, respectively. We introduce two checkerboard patterns Wc and Bc, where Wc has a white pixel at the upper-left position, and Bc is its complement, i.e., the upper-left pixel is black (See Fig. 1). We regard black and white pixels as having a logical value of "1" and "0", respectively.

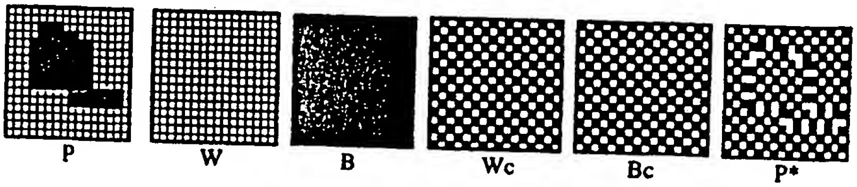


Fig. 1 Illustration of each binary pattern (N=4)

P is interpreted as follows. Pixels in the foreground area have the B pattern, while pixels in the background area have the W pattern. Now we define P* as the conjugate of P which satisfies:

1. The foreground area shape is the same as P.
2. The foreground area has the Bc pattern.
3. The background area has the Wc pattern.

Correspondence between P and P* is one-to-one, onto. The following properties hold true and are easily proved for such conjugation operation. "$\oplus$ "designates the exclusive OR operation.

A) $P^* = P \oplus Wc$

B) $(P^*)^* = P$ (3)

C) $P^* \neq P$ (4)

The most important property about conjugation is the following. (5)

D) Let α (P) be the complexity of a given image P, then we have,

$$\alpha(P^*) = 1 - \alpha(P). \quad (6)$$

It is evident that the combination of each local conjugation (e.g., 8 × 8 area) makes an overall conjugation (e.g., 512 × 512 area).

(6) says that every binary image pattern P has its counterpart P*. The complexity value of P* is always symmetrical against P regarding $\alpha = 0.5$. For example, if P has a complexity of 0.7, then P* has a complexity of 0.3.

2. Criterion to segment a bit-plane into informative and noise-like regions

We are interested in how many binary image patterns are informative and how many patterns are noise-like with regard to the complexity measure α.

Firstly, as we think 8 × 8 is a good size for local area, we want to know the total number of 8 × 8 binary patterns in relation to α value. This means we must check all 2^{64} different 8 × 8 patterns. However, 2^{64} is too huge to make an exhaustive check by any means.

Our practical approach is as follows. We first generate as many random 8 × 8 binary patterns as possible, where each pixel value is set random, but has equal black-and-white probability. Then we make a histogram of all generated patterns in terms of α. This simulates the distribution of 2^{64} binary patterns.

Fig.2 shows the histogram for 4,096,000 8 × 8 patterns generated by our computer. This histogram shape almost exactly fits the normal distribution function as shown in the figure. We would expect this by application of the central limit theorem. The average value of the complexity α was exactly 0.5. The standard deviation was 0.047 in α. We denote this deviation by σ ("sigma" in Fig. 2)

Secondly, our next task is to determine how much image data we can discard without deteriorating the image quality, or, rather at what complexity does the image data become indispensable.

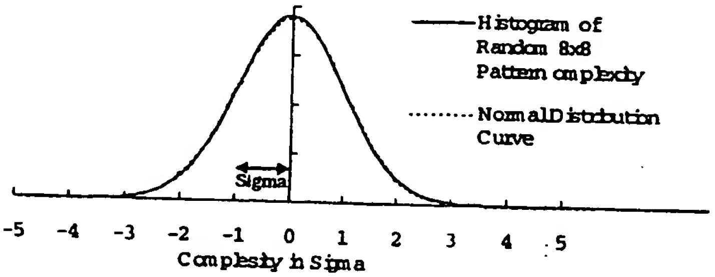


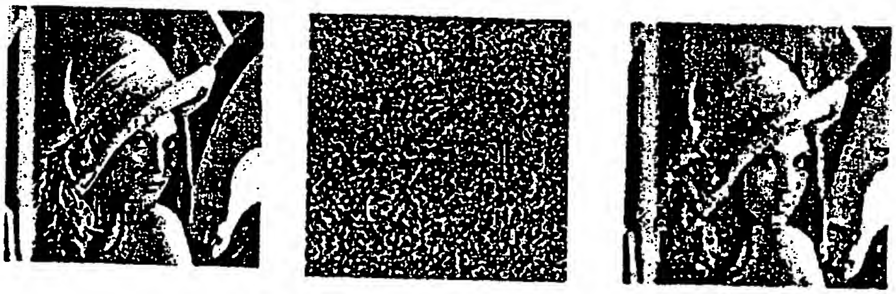
Fig. 2 Histogram of randomly generated 8 × 8 binary patterns

To discard data means to replace local image areas in a bit-plane with random noise patterns. If we replace all the local areas having complexity value $\alpha_L \leq \alpha$, yet the image still maintains good quality, then perhaps we can discard more. If the quality is no longer good, then we can not discard that much. If $\alpha = \alpha_L$ is the minimum complexity value to be good, such α_L is used as the threshold value.

To be indispensable, or rather "informative," for an image means the following. If the image data is still "picture-like" after we have discarded (randomized) a certain amount of image data for such an α that $\alpha \leq \alpha_U$, and if we discard more, then it becomes only noise-like. Then, that α_U is regarded as the limit of the informative image complexity.

If α_L and α_U coincide ($\alpha_0 = \alpha_L = \alpha_U$), we can conclude α_0 is the complexity threshold to divide informative and noise-like regions in a bit-plane.

We made a "random pattern replacing" experiment on a bit-plane of a color image. Fig. 3 illustrates the result.



A) Original image B) Randomization (simple side) C) Randomization (complex side)

Fig. 3 Randomization of the less and the more complex than $\alpha = 0.5 - 8\sigma$.

Fig. 3 shows that if we randomize regions in each bit-plane which are less complex than $0.5 - 8\sigma$, the image can not be image-like any more. While, we can randomize the more complex regions than $0.5 - 8\sigma$ without losing much of the image information.

This means the most of the informative image information is concentrated in between 0 and $0.5 - 8\sigma$ in complexity scale. Surprising enough, it is only 6.67×10^{-14} % of all 8 × 8 binary patterns. Amazingly, the rest (i.e., 99.9999999999999333%) are mostly noise-like binary patterns.

The conclusion of this section is as follows. We can categorize the local areas in the bit-planes of a multi-valued image into three portions (1) Natural informative portions (2) Artificial informative portions (3) Noise-like portions.

The reason we categorize the excessively complicated patterns as "informative" is based on our experiments [7].

4. BPCS STEGANOGRAPHY

Bit-Plane Complexity Segmentation Steganography is our new steganographic technique, which has a large information hiding capacity. As was shown in the previous section, the replacement of the complex regions in each bit-plane of a color image with random binary patterns is invisible to the human eye. We can use this property for our information hiding (embedding) strategy. Our practical method is as follows.

In our method we call a carrier image a "vessel" or "dummy" image. It is a color image in BMP file format, which hides (or, embeds) the secret information (files in any format). We segment each secret file to be embedded into a series of blocks having 8 bytes of data each. These blocks are regarded as 8 x 8 image patterns. We call such blocks the secret blocks. We embed these secret blocks into the vessel image using the following steps.

1. Transform the dummy image from PBC to CGC system.
2. Segment each bit-plane of the dummy image into informative and noise-like regions by using a threshold value (α_0). A typical value is $\alpha_0 = 0.3$.
3. Group the bytes of the secret file into a series of secret blocks.
4. If a block (S) is less complex than the threshold (α_0), then conjugate it to make it a more complex block (S*). The conjugated block must be more complex than α_0 as shown by equation (6).
5. Embed each secret block into the noise-like regions of the bit-planes (or, replace all the noise-like regions with a series of secret blocks). If the block is conjugated, then record this fact in a "conjugation map."
6. Also embed the conjugation map as was done with the secret blocks.
7. Convert the embedded dummy image from CGC back to PBC.

The Decoding algorithm (i.e., the extracting operation of the secret information from an embedded dummy image) is just the reverse procedure of the embedding steps.

The novelty in BPCS-Steganography is itemized in the following.

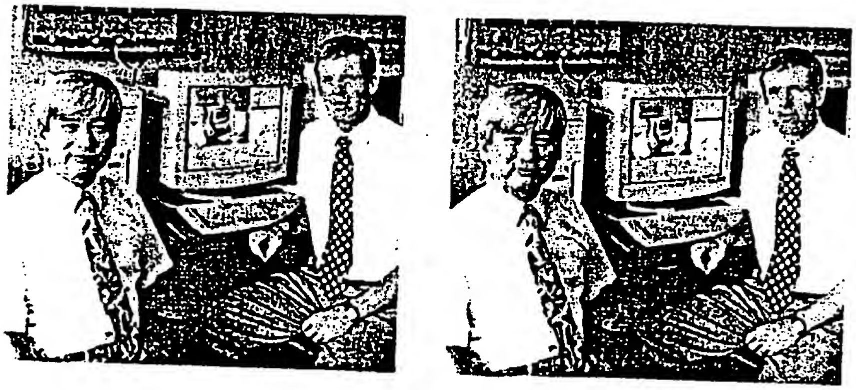
A) Segmentation of each bit-plane of a color image into "Informative" and "Noise-like" regions.
B) Introduction of the B-W boarder based complexity measure (α) for region segmentation
C) Introduction of the conjugation operation to convert simple secret blocks to complex blocks.
D) Using CGC image plane instead of PBC plane

5. EXPERIMENTS

1. Embedding Capacity

We have developed BPCS-Steganography programs for both Windows and Unix. In each program, we took an 8 x 8 square as the local image size. Fig. 4 (A) is an example of the original dummy image (640x588, full color). (B) is the same image with all the information of Fig. 5 embedded in it. As indicated in Fig. 5 this embedded information includes a picture of Lincoln, the text from four historical documents, and the entire script from seven of Shakespeare's plays. Note that the size of the embedded information before compression is almost as great as the image size itself. Furthermore, the embedding operation does not increase the size of the image by even a single byte. Yet, even when viewed on the computer monitor, the images before and after embedding are almost indistinguishable from one another.

It should also be noted that the image of Fig. 4 contains a number of large regions that are relatively flat in color. Our BPCS technique made little use of such regions for embedding, as doing so would introduce noticeable noise in these regions. Fig. 6 presents an example of embedding in a scene with few flat regions. In this case the image is 617x504 pixels. (A) shows the original image, and (B) shows the image after embedding all the information of Fig. 5 plus an additional Shakespearean play, "Antony and Cleopatra" of size 179,900 bytes before compression and 64,184 bytes after. Therefore the total information embedded in this 933,408 byte image is actually 1,212,744 bytes before compression; i.e., the embedded information exceeds the vessel size by 30%! The compressed data size is 505,502 bytes, which is 54% of the vessel size. Even with this much information embedded in the image, the embedded and original images look nearly identical when viewed on the monitor.



(A) Original vessel image

(B) Embedded vessel image

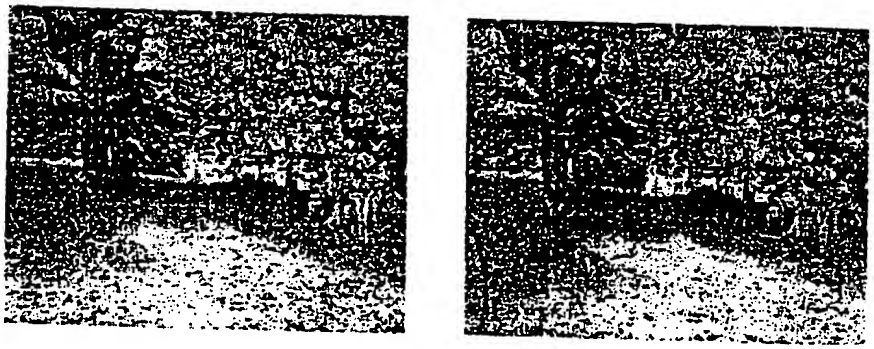
Fig.4 Example of a vessel image

File	Original Size	Compressed Size
Lincoln Picture at right (jpg)	66,190	66,044
The Gettysburg Address	1,502	742
The Declaration of Independence	9,553	4,075
The Constitution (with amendments)	56,989	14,803
The Magna Carta	31,285	12,089
Romeo and Juliet	149,097	58,829
Hamlet	188,626	74,690
Macbeth	109,281	43,698
A Midsummer Night's Dream	99,623	40,242
The Taming of the Shrew	128,385	49,787
The Tempest	102,788	42,044
A Comedy of Errors	89,525	34,275
Total	**1,032,844**	**441,318**

(A) Summary of embedded data

(B) Embedded picture

Fig.5 Files embedded in Fig 4(B)



(A) Original vessel image

(B) Embedded vessel image

Fig.6 Example of a vessel image with fewer flat regions

Through our embedding experiments, we found that most color images taken by a digital camera can be used as vessel images. In almost all cases, the information hiding capacity was nearly 50% of the size of each vessel image. This capacity is 4 to 5 times as large as currently known steganographic techniques.

For a given image, embedding capacity can be traded with image quality by altering the complexity threshold. The image of Fig. 4 used a threshold of 24 border pixels per 8 x 8 region; therefore regions having more border pixels than this were eligible for embedding. Fig. 7 shows how the capacity changes with threshold for this image. For this image a threshold of 24 seemed optimal, while lower thresholds introduced some "noise" to the image.

Threshold	Capacity	Percent Of original
20	499432	44%
25	469480	41%
30	437240	38%
35	400848	35%
40	361800	32%
45	315432	27%

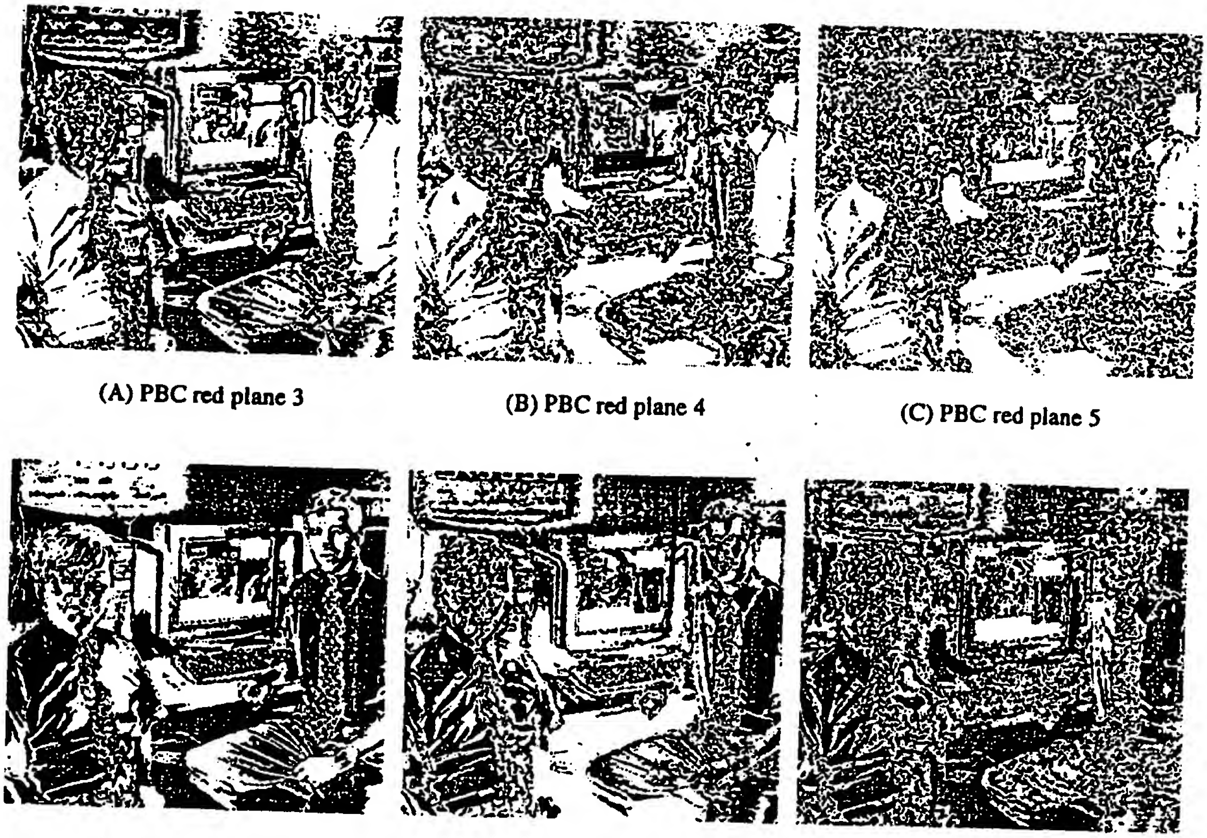
Fig. 7 Capacity vs. Complexity Threshold for the image of Fig. 4

2. Using Gray Coded Bit-Planes for Complexity Segmentation

Fig. 8 illustrates the advantage to using Gray Coded bit planes for complexity segmentation. Parts A through C of this figure show the PBC red bit planes numbered 3 through 5 for the image of Fig. 5a, while parts D through F show the CGC version of these same planes. From looking at such bit planes, one can get a pretty good idea of which regions of the bit plane are complex enough to be replaced with information during BPCS embedding. Recall that the goal with BPCS Steganography is to use as much of the image as possible for hiding information without appreciably altering the visual appearance of the image.

In comparing these two sets of bit planes, it is evident that the PBC bit planes provide a much greater region for embedding. However, substantial portions of the regions on the higher bit planes deemed embeddable using PBC are actually relatively flat in color. For example, note the wall in the background. This is because of the "Hamming Cliffs" which occur with PBC wherein a small change in color affects many bits of the color value. If embedding were to replace the bits in such complex-looking but actually relative flat regions, then substantial color changes would occur. As a simple example, consider a region where the blue value hovers nearly randomly between the binary values of 01111111 and 10000000. In this region, every bit plane would look complex and would thus appear to be embeddable, while in practice, it would be prudent to only embed in the lower one or two planes. Although occurrences such as this where all bits change in a relatively flat region are rare, the frequency of occurrence doubles on each lower bit plane.

CGC images do not suffer from such Hamming Cliffs. Regions which are relatively flat exhibit fewer changes on the higher bit planes. Although this limits the amount of space available for embedding, it does so in regions that should not be altered in the first place. With CGC, embedding in each region is done on the higher bit planes only to the extent allowed by the complexity produced by actual color variation.



(A) PBC red plane 3

(B) PBC red plane 4

(C) PBC red plane 5

(D) CGC red plane 3

(E) CGC red plane 4

(F) CGC red plane 5

Fig. 8 Comparison of PBC and CGC bit planes

6. CUSTOMIZATION OF THE PROGRAM

The BPCS-Steganography algorithm has several embedding parameters for a practical program implementation. Some of them are:

(1) The embedding location of the header(s) of the secret file(s)
(2) The embedding threshold, α_0.
(3) The sequence in which the 8 × 8 regions of the vessel image are considered for embedding.
(4) The encoding of the conjugation map.
(5) Special operations, such as an exclusive-or of the header bytes or embedded data with pseudo-random numbers.
(6) Encryption parameters of the secret file(s)
(7) The compression parameters of the secret file(s)

It is very easy for a single BPCS Steganography program to allow the user to customize parameters such as these, producing a very large number of possible customized programs. In this way, each user or group of users can have their own program that embeds data in an image in a way that is unreadable by others.

7. APPLICATIONS

In discussing applications of BPCS Steganography, it is instructive to note that it differs from digital watermarking in two fundamental ways. The first is that for full color (e.g., 24-bit) images, it has a very large embedding capacity. As described previously, our experiments with BMP images have shown capacities exceeding 50% of the original image size. Although the results presented in this paper are for 24-bit images, we have also been working with other formats, such as 256 color images, which utilize a palette. Although the capacity is lower, the same concepts can be applied.

The second difference is that BPCS Steganography is not robust to even small changes in the image. This can be viewed as a good thing in applications where an unknowing user might acquire an embedded image. Any alteration, such as clipping, sharpening or lossy compression, would "destroy the evidence" and make it unusable for later extraction. Extracting the embedded information requires a deliberate attempt by a knowledgeable user on an unaltered image. The lack of robustness also ties in to the fact that a malicious user cannot alter the embedded data without knowledge of the customization parameters.

The more obvious applications of BPCS Steganography relate to secret communications. For example a person, group, or company can have a web page containing secret information meant for another. Anyone can download the web page, so when the intended recipient does so, it does not draw any attention. Extracting the embedded information would require software customized with the proper parameters. Encryption of the embedded data would further improve security. This scenario is analogous to putting something in a very secure safe and then hiding the safe in a hard to find place.

In some applications, the presence of the embedded data may be known, but without the customization parameters, the data is inseparable from the image. In such cases, the image can be viewable by regular means, but the data is tied to the image and can't readily be replaced with other data. Others may know the data is there, but without the customization parameters, they cannot alter it and still make it readable by the customized software.

Applications of BPCS Steganography are not limited to those related to secrecy. For such applications, the presence of the embedded data may be known, and the software for extraction and embedding can be standardized to a common set of customization parameters. An example of this is a digital photo album, where information related to a photo, such as date and time taken, exposure parameters, and scene content, can be embedded in the photo itself.

8. CONCLUSIONS AND FUTURE WORK

The objective of this paper was to demonstrate our BPCS-Steganography, which is based on a property of the human visual system. The most important point for this technique is that humans can not see any information in the bit-planes of a color image if it is very complex. We have discussed the following points and showed our experiments.

(1) We can categorize the bit-planes of a natural image as informative areas and noise-like areas by the complexity thresholding.
(2) Humans see informative information only in a very simple binary pattern.
(3) We can replace complex regions with secret information in the bit-planes of a natural image without changing the image quality. This leads to our BPCS-Steganography.
(4) Gray coding provides a better means of identifying which regions of the higher bit planes can be embedded.
(5) A BPCS-Steganography program can be customized for each user. Thus it guarantees secret Internet communication.

We are very convinced that this steganography is a very strong information security technique, especially when combined with encrypted embedded data. Furthermore, it can be applied to areas other than secret communication. Future research will include the application to vessels other than 24-bit images, identifying and formalizing the customization parameters, and developing new applications.

9. ACKNOWLEDGEMENT

This project is partly funded by the Advanced Information Technology Program (AITP) of Information-technology Promotion Agency (IPA), Japan.

10. REFERENCES

1. Hall, Ernest L., *Computer Image Processing and Recognition*, Academic Press, New York, 1979.
2. Jain, Anil K., *Fundamentals of Digital Image Processing*, Prentice Hall, Englewood Cliffs, NJ, 1989.
3. Kawaguchi, E., Endo, T. and Matsunaga, J., "Depth-first picture expression viewed from digital picture processing", *IEEE Trans. on PAMI*, vol.5, no.4, pp.373-384, 1988.
4. Kawaguchi, E. and Taniguchi, R., "Complexity of binary pictures and image thresholding - An application of DF-Expression to the thresholding problem", *Proceedings of 8th ICPR*, vol.2, pp.1221-1225, 1986.
5. Kawaguchi, E. and Taniguchi, R., "The DF-Expression as an image thresholding strategy", *IEEE Trans. on SMC*, vol.19, no.5, pp.1321-1328, 1989.
6. Kamata, S, Eason, R. O., and Kawaguchi, E., "Depth-First Coding for multi-valued pictures using bit-plane decomposition", *IEEE Trans. on Comm.*, vo.43, no.5, pp.1961-1969, 1995.
7. Kawaguchi, E. and Niimi M, "Modeling Digital Image into Informative and Noise-Like Regions by Complexity Measure", Preprint of the 7th *European-Japanese Conference on Information Modeling and Knowledge Bases*, pp.268-278, May, Toulouse, 1997.

PROCEEDINGS OF SPIE

SPIE—The International Society for Optical Engineering

Multimedia Systems and Applications

Andrew G. Tescher
Bhaskaran Vasudev
V. Michael Bove, Jr.
Barbara Derryberry
Chairs/Editors

2–4 November 1998
Boston, Massachusetts

SPIE
P
PROCEEDINGS SERIES

Volume 3528

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 February 2002 (14.02.2002)

PCT

(10) International Publication Number
WO 02/13436 A1

(51) International Patent Classification⁷: H04K 1/02

(21) International Application Number: PCT/US01/24468

(22) International Filing Date: 2 August 2001 (02.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/634,506 9 August 2000 (09.08.2000) US

(71) Applicant: AVWAY.COM INC. [US/US]; 12 Broad Street, Red Bank, NJ 07701 (US).

(72) Inventors: RAMKUMAR, Mahalingam; Apartment 4A, 55 Belgrove Drive, Kearny, NJ 07032 (US). AKANSU, Ali, N.; 181 Heights Terrace, Middletown, NJ 07032 (US).

(74) Agent: GREELEY, Paul, D.; Ohlandt, Greeley, Ruggiero & Perle, L.L.P., 10th floor, One Landmark Square, Stamford, CT 06901-2682 (US).

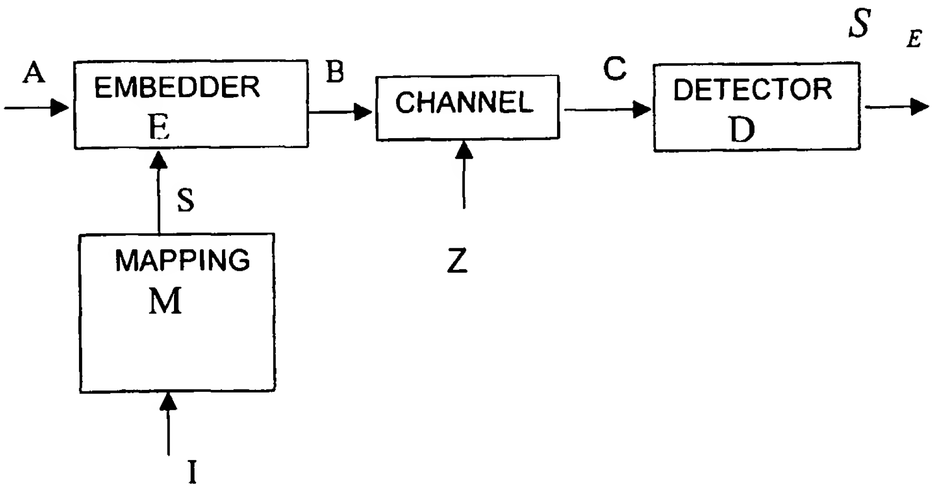
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR STEGANOGRAPHICALLY EMBEDDING INFORMATION BITS IN SOURCE SIGNALS



(57) Abstract: A method and system for embedding (E) information bits in a source signal (A) like images, audio or video. The embedding being performed optimally for a given worst-case scenario of unintentional or intentional attack of the host signal (to remove the embedded bits), and a given distortion of the host signal due to information embedding.

METHOD AND SYSTEM FOR STEGANOGRAPHICALLY EMBEDDING INFORMATION BITS IN SOURCE SIGNALS

This invention relates to a method and system for embedding information bits in a host signal. The embedding may be performed to determine origin of any perfect or imperfect copies of the composite (host plus message) signal, or to use the host signal as a cover for secret or covert communications, over a channel which is primarily meant for transmitting the host signal only.

BACKGROUND OF THE INVENTION

Data hiding or steganography is the art of hiding a message signal in a host signal, without any perceptual distortion of the host signal. The composite (host plus message) signal is also referred to as stego-signal. Though steganography is often confused with the relatively well-known cryptography, the two are but loosely related. Cryptography is about hiding the contents of a message. Steganography, on the other hand, is about concealing the very fact that a message is hidden. Steganography may be considered as communication through subliminal channels, or secret communication.

Rapid increases in bandwidth available for dissemination and storage of digital content and availability of software tools for editing multimedia content, such as, video, images or audio calls for systems and methods to establish origin of such content. In addition, large volumes of multimedia content being exchanged over insecure channels, such as, the Internet, provide within themselves secure and subliminal steganographic channels for secure or secret communications.

The proliferation of digital multimedia as opposed to conventional analog forms, is primarily a result of (1) the ease with which digital data can be exchanged over the Internet, and (2) the emergence of efficient multimedia data compression techniques.

The first reason listed above is also a major cause for concern. Unlimited perfect copies of the original content can be made, and distributed easily. It was this concern of protecting intellectual property rights of multimedia data in digital form, that primarily triggered researchers to find ways to watermark multimedia data. Watermarking the content is done by embedding some data in the host signal (original content). The embedded data may be an imperceptible signature, which the owner of the multimedia content should be able to extract when a dispute regarding ownership occurs.

Data hiding in multimedia could help in providing proof of origin and distribution of content. Multimedia content providers would be able to communicate with the compliant multimedia players (or renderers) through the subliminal, steganographic channel. This communication may control or restrict access of multimedia content, and carry out e-commerce for pay-per-use implementations.

A typical application of data hiding for multimedia content delivery may involve the content providers supplying the raw multimedia data (say a full length movie) along with some hidden agents or control data . The job of the distributors would be to package the content in some suitable format (such as, MPEG) understandable by the player, for distribution of the multimedia through DVDs/CDs or live digital broadcasts, or by hosting web sites for downloads or streaming. The compliant multimedia players, will typically be connected to the Internet.

In conventional multimedia distribution, the content provider looses all control over how the multimedia is used/abused the moment it is acquired by another party. The key idea behind data hiding is to re-establish control whenever the content is used. The content provider, by hiding an agent in his raw data, hopes to control access to his/her multimedia content. This can be done with the co-operation of the players, and an established protocol for communication between the content providers and the compliant multimedia players.

Data hiding can be broadly classified into two categories depending on whether the original content is needed for extraction of the hidden bits: (1) non-oblivious methods need the original content for extracting the hidden bits; and (2) on the other hand, oblivious detection methods extract the hidden bits without any knowledge of the original.

In most data hiding methods, sequence of bits to be embedded, viz. B, is converted to a form suitable for embedding in a cover content. Initially, the bit sequence is converted to a signature sequence. Thereafter, the signature sequence is embedded in the cover content by an embedding function to obtain the stego-content.

From a signal processing perspective; data hiding methods can be classified into two categories, depending on the type of embedding and detecting operators. The first category includes methods where the embedding function adds the signature sequence linearly to stego-content, and the detector detects from the stego-content via correlative processing (these methods are referred to as Type I methods in data hiding literature). In the second category the embedding function and the detector are non-linear, typically employing quantizers (these methods are referred to as Type II methods in data hiding literature). One of the important characteristics of the non-linear methods is their ability to suppress the noise due to the original content (or self-noise), even though the original content is not available at the receiver.

The present invention provides a unique data hiding technique that substantially reduces the effect that noise, distortion or corruption of the host signal have on the detected signal so as to greatly enhance the integrity of steganography techniques employing oblivious detection of the hidden data. The crux of the invention is a class of methods referred to as Type III methods of which Types I and II are just special cases. An optimal choice of parameters for the proposed Type III methods depending on the engineering constraints, can substantially improve the performance of data hiding.

The present invention also provides many additional advantages, which shall become apparent as described below.

SUMMARY OF THE INVENTION

A method for embedding a message signal in a host signal, the method comprising the steps of:

(a) embedding the message signal into the host signal, thereby producing a stego signal; and

(b) detecting an estimate of the message signal from the stego signal; provided that the detecting step (b) is not an exact inverse of the embedding step (a), and the host signal cannot be exactly extracted from the stego signal.

The embedding step (a) produces a value b_i in the stego signal from a value a_i in the host signal, and wherein the embedding step (a) comprises limiting to a limit value $\frac{\beta}{2}$, a magnitude of difference between b_i and a_i.

Furthermore, the embedding step (a) employs a continuous periodic function to produce the stego signal, and wherein the detecting step (b) employs a continuous periodic function to produce the estimated message signal. The continuous periodic function is a triangular function $f(x)$ having a period Δ, wherein:

$$-\frac{\Delta}{4} \le f(x) \le \frac{\Delta}{4} \text{ for all x;}$$

$$f(0) = -\frac{\Delta}{4}; \quad \text{and}$$

$$f(\frac{\Delta}{2}) = \frac{\Delta}{4}$$

Optionally, the embedding step (a) produces a value b_i in the stego signal from a value a_i in the host signal and a value s_i in the message signal, such that the embedding step (a):

(i) is subject to a maximum distortion constraint P,

(ii) employs a continuous periodic function having a period Δ, and

(iii) is represented by the function $b_i = E(a_i, s_i)$, and employs an algorithm as follows:

if $rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}$, then $p_i = 3\frac{\Delta}{4} - rem(\frac{a_i}{\Delta})$,

else $p_i = rem(\frac{a_i}{\Delta}) - \frac{\Delta}{4}$;

$e_i = s_i - p_i$;

if $(|e_i| > \frac{\beta}{2})$, then $e_i = sign(e_i)\frac{\beta}{2}$;

$q_i = rem(\frac{a_i}{\Delta})$;

if $q_i > \frac{\Delta}{2}$, then $e_i = -e_i$;

if $a_i > 0$, then $b_i = a_i + e_i$,

else $b_i = a_i - e_i$.

The method of the present invention is particularly useful when the stego signal is corrupted or distorted prior to detecting step (b). In this embodiment where the stego signal is corrupted a value b_i in the stego signal is modified after the embedding step (a) to yield a value c_i in the corrupted or distorted stego signal, such that the detecting step (b):

(i) produces a value s_{ei} in the estimated message signal from a value c_i in a distorted stego signal,

(ii) employs a continuous periodic function having a period Δ, and

(iii) is represented by the function $s_{ei} = D(c_i)$, and employs an algorithm as follows:

$q_i = rem(\frac{c_i}{\Delta})$;

if $q_i > \frac{\Delta}{2}$, then $s_{ei} = 3\frac{\Delta}{4} - q_i$,

else $s_{ei} = q_i - \frac{\Delta}{4}$.

Preferably the host signal is a sequence a_i, for $i=1$ to N; the message signal is a sequence s_i, for $i=1$ to N; the stego signal is a sequence b_i, for $i=1$ to N; the corrupted or distorted stego signal is a sequence c_i, for $i=1$ to N; and the estimated message signal is a sequence s_{ei}, for $i=1$ to N.

The embedding step (a) preferably (i) imposes a limit $\frac{\beta}{2}$ on a magnitude difference between a value b_i in the stego signal that is produced from a value a_i in the host signal; and (ii) employs a continuous periodic function having a period Δ to produce the stego signal, wherein such the limit $\frac{\beta}{2}$ and the period Δ are chosen to minimize a mean square distance between the message signal and the estimated message signal, subject to a maximum distortion constraint P of the embedding step (a).

The present invention also provides a method for mapping K information bits to a message signal s_i, $i=1$ to N. This method comprising the step of: grouping the K information bits together to represent one of 2^L symbols, wherein each of the 2^L symbol is mapped to a basis vector or its negative of a $2^{L-1}\times 2^{L-1}$ orthogonal transform matrix. The orthogonal transform matrix is obtained from a cyclic all-pass filter and its circular shifts. The cyclic all-pass filter is preferably obtained from a key.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of the data embedding, channel and detection operation according to the present invention;

Fig. 2 is a graph depicting a periodic triangular function employed by the detector D of Fig. 1;

Fig. 3(a) is a graph demonstrating that the distortion introduced during the embedding the S in A (to obtain B) of Fig. 1 in accordance with Type II will be uniformly distributed between $-\frac{\Delta}{2}$ and $+\frac{\Delta}{2}$;

Fig. 3(b) is a graph depicting the distribution of the distortion introduced in accordance with the method of the present invention; and

Fig. 3(c) is a graph depicting the distribution of the limiting noise t_i.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The present invention is a method for efficient secure communication over subliminal channels provided by multimedia host signals like audio, images and video transmitted over any channel. For example, the host signal may be transmitted over the Internet or distributed in storage mediums by other means or even transmitted over analog channels, such as, that used for analog television or radio broadcasts. Typically the host signal is expected to undergo some distortion before it reaches one or many end points where it may be stored or rendered.

In the method described herein, the host signal may be any form of naturally occurring signals, such as, audio, image or video or artificially synthesized versions of them. The host signal may further be represented in some transform domain. The choice of the transform may depend on the nature of the application. For example, if the host signal is an image and is not expected to be re-scaled, resized or rotated, any unitary transform may be used. On the other hand, if the image is likely to undergo rotation, scaling and/or translation, a Rotation-Scale-Translation invariant transform may be used. If the image is cropped, data embedding may be performed in many blocks of the image, so that the hidden bits can be extracted even if one such block survives. In general, the host signal can be coefficients of a one-to-one transform or a many-to-one transform.

In the method described herein, the host signal can therefore be considered as a vector or a sequence of N real or complex numbers, represented by

$$A = [a_1 \quad a_2 \quad \cdots \quad a_N].$$

A sequence of K bits, represented by

$$I = [i_1 \quad i_2 \quad \cdots \quad i_K],\ i, j = 1/0 \text{ for } 1 \le j \le K$$

is mapped by a mapping M to a signature sequence S,

$$M : I \to S, \text{ where}$$

$$S = [s_1 \quad s_2 \quad \cdots \quad s_N]$$

An embedder E embeds the sequence in A to obtain the stego sequence B, $B = E(A,S)$, where

$$B = [b_1 \quad b_2 \quad \cdots \quad b_N],$$

the embedding being performed element-wise,

$$\begin{aligned} b_1 &= E(a_1, s_1) \\ b_2 &= E(a_2, s_2) \\ b_3 &= E(a_3, s_3) \\ &\vdots \\ b_N &= E(a_N, s_N) \end{aligned}$$

subject to the constraint that $d(A,B) \le P$ where $d(A,B)$ is some distance measure of signals A and B, and P is the maximum permitted distortion of the host signal. In the preferred embodiment the distance measure is the mean square error:

$$d(A,B) = \frac{(a_1 - b_1)^2 + (a_2 - b_2)^2 + \cdots + (a_N - b_N)^2}{N}$$

The stego sequence B may undergo some distortion before it reaches the detector as C, given by $C = B + Z$, where

$$Z = [z_1 \quad z_2 \quad \cdots \quad z_N],$$

is the noise in the channel used for transmitting the host signal, and

$$C = [c_1 \quad c_2 \quad \cdots \quad c_N].$$

The detector D obtains an estimate S_e of the signature sequence S embedded:

$$S_e = D(C).$$

The block diagram of data embedding, the channel and detection operation is shown in FIGURE 1.

Based on this generalization of the embedding and detecting functions E and D, prior art in this field can be categorized into two types.

Characteristics of Type I

- $B = E(A,S) \to B = A + S$
- $D(B) = A + S \neq S$

The above two equations imply that E and D are not inverses.
In addition, if S is known one can obtain the original host sequence A from B as $A = B - S$.

Characteristics of Type II

- $B = E(A,S)$
- $D(B) = S$

Unlike Type I methods, the above two equations show that for Type II methods E and D are exact inverses. Additionally, unlike Type I methods, it is not possible to obtain A exactly, given B and S.

In the core of this invention is a class of embedding and detection operators E and D, we shall refer to as Type III.

Characteristics of Type III

- $B = E(A,S)$
- $D(B) \neq S$

The above two equations illustrate that E and D are not exact inverses (like Type I and unlike Type II). Further, given S and B it is not possible to obtain A (like Type II and unlike Type I).

In a preferred embodiment described herein, the detector D, where

$$S_e = D(C),\ S_e = [s_{e1} \quad s_{e2} \quad \cdots \quad s_{eN}\ ]$$

is implemented by the following algorithm:

$$q_i = rem(\frac{c_i}{\Delta});$$

$$\text{if } q_i > \frac{\Delta}{2} \text{ then } s_{ei} = 3\frac{\Delta}{4} - q_i,$$

$$\text{else } s_{ei} = q_i - \frac{\Delta}{4}.$$

In the above algorithm, rem (x) stands for the remainder of a division operation (x). For example,

rem(5/4)=1, rem(2/2)=0, rem(-6/4)=rem(6/4)=2.

The choice of the parameter Δ is dictated by the distortion constraint P and the energy of the channel noise Z. The detector may also be thought of as employing a periodic triangular function shown in FIGURE 2,

$$y = f(x) = f(x + m\Delta) \text{ for integer } m. \text{ Also,}$$

$$-\frac{\Delta}{4} \le f(x) \le \frac{\Delta}{4} \text{ for all x,}$$

and specifically,

$$f(0) = -\frac{\Delta}{4}$$

$$f(\frac{\Delta}{2}) = \frac{\Delta}{4}$$

The embedding operation $b_i = E(a_i, s_i)$ is implemented by the following algorithm:

$$\text{if } rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}, \text{ then } p_i = 3\frac{\Delta}{4} - rem(\frac{a_i}{\Delta}),$$

```
else $p_i = rem(\frac{a_i}{\Delta}) - \frac{\Delta}{4}$;
$e_i = s_i - p_i$;
if $(|e_i| > \frac{\beta}{2})$, then $e_i = sign(e_i)\frac{\beta}{2}$;
if $rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}$, then $e_i = -e_i$;
if $a_i > 0$, then $b_i = a_i + e_i$,
else $b_i = a_i - e_i$.
```

In the above algorithm, β is a parameter, the choice of which is dictated by the distortion constraint P and the energy of the channel noise Z. Also sign (x) equals +1 if the quantity 'x' is positive and sign (x) equals –1 if the quantity 'x' is negative. For example,

sign(-20) = sign(-1) = -1, and sign(11) = sign(1) = +1.

As an example of the embedding and detection operations, let

A=[-65, –250, 19, 43, –172, 179, 178, –6], and
S=[10, 10, –10, 10, –10, 10, –10, 10],
$\Delta = 40$, and $\beta = 10$ (Note that $-\frac{\Delta}{4} \le s_i \le \frac{\Delta}{4}$ for all i).

Now $B = E(A,S)$ is given by

B=[-60, –255, 14, 48, –167, 180, 173, –11]. Let
Z=[-4, –8, 2, –10, –5, 3, –6, -4]. Therefore,
C=B+Z=[-64, –263, 16, 38, –172, 183, 167, –15], and

$S_e = D(C)$ is now

$S_e = [6, 7, 6, -8, 2, 7, -3, 5]$.

Now let us consider $b_i = E(a_i, s_i)$, for i=1. $a_1 = -65, s_1 = 10$.

If $rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}$, then $p_i = 3\frac{\Delta}{4} - rem(\frac{a_i}{\Delta})$,

$rem(\frac{-65}{40}) = 25 \ge \frac{\Delta}{2}$, $p_1 = 30 - 25 = 5$

else $p_i = rem(\frac{a_i}{\Delta}) - \frac{\Delta}{4}$

$e_i = s_i - p_i$ $\qquad e_1 = 10 - 5 = 5$

if $(|e_i| > \frac{\beta}{2})$, then $e_i = sign(e_i)\frac{\beta}{2}$ $\qquad e_1 = \frac{\beta}{2}$

if $rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}$ $e_i = -e_i$ $\qquad rem(\frac{-65}{40}) = 25 > \frac{\Delta}{2}, e_1 = -5$

if $a_i > 0$ $b_i = a_i + e_i$

else $b_i = a_i - e_i$ $\qquad \underline{b_1 = -65 - (-5) = -60}$

Now $c_1 = b_1 + z_1 = -60 - 4 = -64$. For detection,

$q_i = rem(\frac{c_i}{\Delta})$. $\qquad q_1 = rem(\frac{-64}{40}) = 24$

if $q_i > \frac{\Delta}{2}$ then $s_{ei} = 3\frac{\Delta}{4} - q_i$ $\qquad \underline{q_1 = 24 > 20, s_{e1} = 30 - 24 = 6}$

else $s_{ei} = q_i - \frac{\Delta}{4}$

For Type II systems ($\Delta = \beta$) the distortion introduced, viz. $B - A$ for embedding the S in A (to obtain B) will be uniformly distributed between $-\frac{\Delta}{2}$ and $+\frac{\Delta}{2}$ (FIGURE 3a), and the average energy of the distortion introduced in A will be $\frac{\Delta^2}{12}$. For Type III systems, the distribution of the distortion introduced is depicted in FIG. 3b. The average energy of the distortion for a Type III system is given by

$$\frac{\beta^2(3\Delta - 2\beta)}{12\Delta}.$$

While for Type II systems $s_i = D(b_i)$, for the proposed Type III system

$$D(b_i) - s_i = t_i$$

where t_i is noise due to "limiting" (limiting occurs when $\beta < \Delta$). The distribution of the limiting noise t_i is shown in FIG. 3c, and the average energy of the limiting noise is given by

$$\frac{(\Delta-\beta)^3}{12\Delta}.$$

Optimal choice of the parameters Δ and β for a given signal-to-noise ratio (snr)

$$\text{snr} = \frac{\text{Signal Energy}}{\text{Noise Energy}} = \frac{P = \dfrac{\beta^2(3\Delta-2\beta)}{12\Delta}}{\text{Energy of Channel Noise } Z}$$

is shown in Table 1. In Table 1,

$\text{SNR} = 10\log_{10}(\text{snr})\,\text{dB}$, and

$$k = \frac{\Delta}{\sqrt{\dfrac{P}{12}}}$$

From the values of Δ and signal energy P, β can be obtained by solving

$$\frac{\beta^2(3\Delta-2\beta)}{12\Delta} = P$$

Table 1 – Optimal Choice of k for different SNRs

SNR	k
4.77	1.24
3.01	1.40
1.76	1.55
0.00	1.87
-3.01	2.57
-4.77	3.14
-6.02	3.59
-6.99	4.04
-7.78	4.40
-8.45	4.78

-9.03	5.11
-9.54	5.41
-10.00	5.71
-13.01	8.10
-14.77	9.95

The optimal parameters are chosen to minimize

$$J = \frac{(s_1 - s_{e_1})^2 + (s_2 - s_{e_2})^2 + \cdots + (s_N - s_{e_N})^2}{\Delta^2},$$

which is the normalized mean square distance between the embedded signature sequence and the detected signature sequence. The minimization performed under the assumption that the channel noise Z has a Gaussian distribution. If Z is zero mean and has a variance of σ_z^2, then

$$J = \frac{1}{\Delta^2} \sum_{i=0}^{\infty} \int_{\frac{i\Delta}{2}}^{\frac{(i+1)\Delta}{2}} \left(\frac{(2i+1)\Delta}{4} - z \right)^2 f_Z(z) \mathrm{d}z,$$

where

$$f_Z(z) = \frac{\beta}{2\sqrt{2\pi\sigma_z^2}} \mathrm{e}^{-\frac{z^2}{2\sigma_z^2}} + \frac{1}{2\Delta} \left\{ \mathrm{erf}\left(\frac{z + \frac{\Delta - \beta}{2}}{\sqrt{2}\sigma_z} \right) - \mathrm{erf}\left(\frac{z - \frac{\Delta - \beta}{2}}{\sqrt{2}\sigma_z} \right) \right\},$$

and

$$\mathrm{erf}(t) = \frac{2}{\pi} \int_0^t \mathrm{e}^{-\frac{y^2}{2}} \mathrm{d}y$$

The mapping

$$M : I \rightarrow S,$$

in the preferred embodiment takes the following form. The bit sequence I of K bits is grouped into K/L L-bit symbols. Each L-bit symbol will be mapped to one of in 2^{L-1} basis vectors of an orthogonal transform. Thus we can embed $\frac{N}{2^{L-1}}$ symbols or $\frac{NL}{2^{L-1}}$ bits in the sequence A. For example, if N=8192, for

L = 2, 3, 4, 5, 6, 7, 8, 9, and 10,

K = 8192, 6144, 4096, 2560, 1536, 896, 512, 288, and 160 bits respectively.

In the preferred embodiment, L bits corresponding to each symbol are assumed to represent a decimal number between 1 and 2^{L-1}. This number is used as the index of the basis vector to be chosen.

The basis vectors of a $Q \times Q$ orthogonal transform where $Q = 2^{L-1}$ are obtained from a random seed as follows. The random seed (or key) is used to generate uniformly distributed random sequence

$$[\theta_1, \ \theta_2, \ \cdots \ , \theta_{(\frac{Q}{2}-1)}], -\pi \leq \theta_i \leq \pi .$$

The $\frac{Q}{2}-1$ random numbers define the phase of the discrete Fourier transform (DFT) of a sequence H. The magnitudes of the discrete Fourier coefficients are assumed to be unity. Such a sequence H is cyclic all-pass of length Q. H is orthogonal to all its cyclic shifts. Such a sequence derived from a random seed and all its cyclic shifts form a complete basis, and can therefore be considered as the basis vectors of a $Q \times Q$ unitary transform matrix.

As an example, let Q=8. Let the $\frac{Q}{2}-1$=3 random numbers be

[-2.7489, –0.7854, 1.1781].

These random numbers describe are the angles of the Discrete Fourier Transform coefficients of H. The angles of the 8 coefficients of H are

[0, –2.7489, –0.7854, 1.1781, 0, –1.1781, 0.7584, 2.7489]

and their magnitudes are equal to 1. The cyclic all-pass filter H is obtained by inverse Discrete Fourier Transform as

[0.2915, –0.1499, 0.3999, –0.0415, 0.5621, 0.5034, –0.2534, –0.3121]

Each segment of length Q of the signature sequence S of length N carries information pertaining to one symbol between 0 and 2Q-1.

Symbol sequence - $[y_1, \quad y_2, \quad \cdots \quad , y_{\frac{N}{Q}}]$; $0 \le y_i \le 2Q-1$ for all i

Signature sequence - $[S_1, \quad S_2, \quad \cdots \quad , S_{\frac{N}{Q}}] = S$

The algorithm for obtaining the signature sequence is as follows

```
for all i
 sign=1;
 if $y_i \ge Q$
 shift = $y_i - Q$;
 sign = -1;
 else
 shift = $y_i$;
 circularshift (sign x H, shift);
```

For example, if

H = [0.2915, –0.1499, 0.3999, –0.0415, 0.5621, 0.5034, –0.2534, –0.3121]

and $y_i = 2$ (circular shift by 2) then,

S_i = [-0.2534, –0.3121, 0.2915, –0.1499, 0.3999, -0.0415, 0.5621, 0.5034].

As an other example, if $y_i = 10$ (circular shift by 10-8=2 followed by negation), then

S_i = [0.2534, 0.3121, -0.2915, 0.1499, -0.3999, 0.0415, -0.5621, -0.5034].

The Algorithm for the inverse mapping $M^{-1} : S_e \to I_e$ is as follows:

Each segment of length Q of the detected sequence $S_e = [S_{e1}, \quad S_{e2}, \quad \cdots \quad , S_{e\frac{N}{Q}}]$ corresponds to a symbol. The embedded symbol is estimated as follows:

HH=DFT(H)

```
for all i
SS=DFT($S_{ei}$);
YY=IDFT(SS.*HH);
$y_{ei}$=index(max(abs(YY)));
 if (YY[$y_{ei}$]) < 0, then
$y_{ei}$=$y_{ei}$+Q
```

In the above algorithm, DFT stands for Discrete Fourier Transform and IDFT stands for Inverse DFT. y_{ei} is the estimate of y_i, which is the symbol embedded in the i'th segment of S. Finally, the binary representation of e y_{el} yields the corresponding sequence of bits I_{ei}, and

$$I_e = [I_{e1}, \quad I_{e2}, \quad \cdots \quad ,I_{e\frac{N}{Q}}].$$

I_e is the estimate of the hidden bit sequence I.

WHAT IS CLAIMED IS:

1. A method for embedding a message signal in a host signal, said method comprising the steps of:
   (a) embedding said message signal into said host signal, thereby producing a stego signal; and
   (b) detecting an estimate of said message signal from said stego signal; provided that said detecting step (b) is not an exact inverse of said embedding step (a), and said host signal cannot be exactly extracted from said stego signal.

2. The method according to claim 1, wherein said stego signal is corrupted or distorted prior to detecting step (b).

3. The method according to claim 1, wherein said embedding step (a) produces a value b_i in said stego signal from a value a_i in said host signal, and wherein said embedding step (a) comprises limiting to a limit value $\frac{\beta}{2}$, a magnitude of difference between b_i and a_i.

4. The method according to claim 1, wherein said embedding step (a) employs a continuous periodic function to produce said stego signal, and wherein said detecting step (b) employs said continuous periodic function to produce said estimated message signal.

5. The method according to claim 4, wherein said continuous periodic function is a triangular function.

6. The method according to claim 5, wherein said triangular function $f(x)$ has a period Δ, and

   wherein:

$$-\frac{\Delta}{4} \le f(x) \le \frac{\Delta}{4} \text{ for all x;}$$

$f(0) = -\frac{\Delta}{4}$; and

$f(\frac{\Delta}{2}) = \frac{\Delta}{4}$.

7. The method according to claim 1, wherein said embedding step (a) produces a value b_i in the said stego signal from a value a_i in said host signal and a value s_i in said message signal, such that said embedding step (a):

   (i) is subject to a maximum distortion constraint P,

   (ii) employs a continuous periodic function having period Δ, and

   (iii) is represented by the function $b_i = E(a_i, s_i)$, and employs an algorithm as follows:

```
if $rem(\frac{a_i}{\Delta}) > \frac{\Delta}{2}$, then $p_i = 3\frac{\Delta}{4} - rem(\frac{a_i}{\Delta})$,
else $p_i = rem(\frac{a_i}{\Delta}) - \frac{\Delta}{4}$;
$e_i = s_i - p_i$;
if $(| e_i |> \frac{\beta}{2})$, then $e_i = sign(e_i)\frac{\beta}{2}$;
$q_i = rem(\frac{a_i}{\Delta})$;
if $q_i > \frac{\Delta}{2}$, then $e_i = -e_i$;
if $a_i > 0$, then $b_i = a_i + e_i$;
else $b_i = a_i - e_i$.
```

8. The method according to claim 2, wherein a value b_i in said stego signal is modified after said embedding step (a) to yield a value c_i in said corrupted or distorted stego signal, and wherein said detecting step (b):

   (i) produces a value s_{ei} in said estimated message signal from a value c_i in said distorted stego signal,

   (ii) employs a continuous periodic function having a period Δ, and

(iii) is represented by the function $s_{ei} = D(c_i)$, and employs an algorithm as follows:

$$q_i = rem(\frac{c_i}{\Delta});$$

$$\text{if } q_i > \frac{\Delta}{2}, \text{ then } s_{ei} = 3\frac{\Delta}{4} - q_i,$$

$$\text{else } s_{ei} = q_i - \frac{\Delta}{4}.$$

9. The method according to claim 2, wherein

said host signal is a sequence a_i, for $i = 1$ to N;

said message signal is a sequence s_i, for $i = 1$ to N;

said stego signal is a sequence b_i, for $i = 1$ to N;

said corrupted or distorted stego signal is a sequence c_i, for $i = 1$ to N; and

said estimated message signal is a sequence s_{ei}, for $i = 1$ to N

10. The method according to claim 1, wherein said embedding step (a):

(i) imposes a limit $\frac{\beta}{2}$ on a magnitude difference between a value b_i in said stego signal that is produced from a value a_i in said host signal;

(ii) employs a continuous periodic function having a period Δ to produce said stego signal, wherein such said limit $\frac{\beta}{2}$ and said period Δ are chosen to minimize a mean square distance between said message signal and said estimated message signal, subject to a maximum distortion constraint P of said embedding step (a).

11. A method for mapping K information bits to a message signal s_i, $i = 1$ to N, said method comprising the steps of:

grouping said K information bits together to represent one of 2^L symbols, wherein each said 2^L symbol is mapped to a basis vector or its negative of a $2^{L-1} \times 2^{L-1}$ orthogonal transform matrix.

12. The method according to claim 11, wherein said orthogonal transform matrix is obtained from a cyclic all-pass filter and its ciruclar shifts.

13. The method according to claim 12, wherein said cyclic all-pass filter is obtained from a key.

FIGURE 1

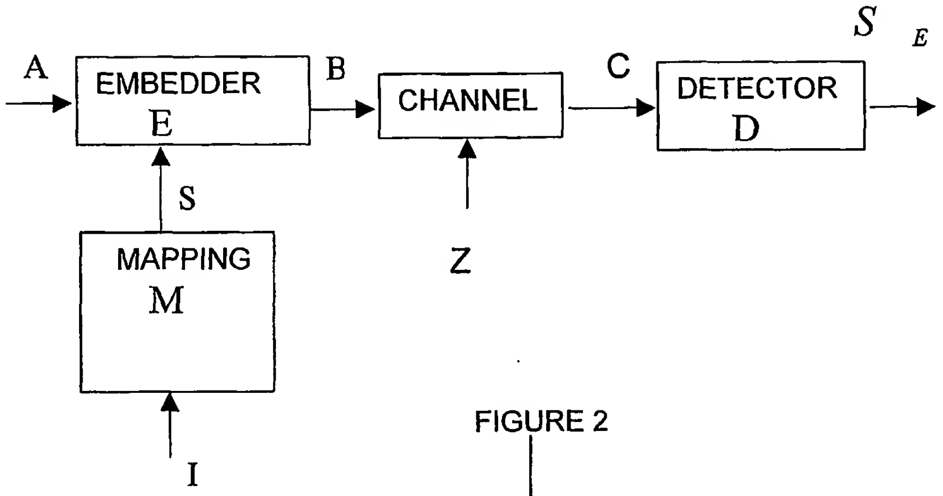


FIGURE 2

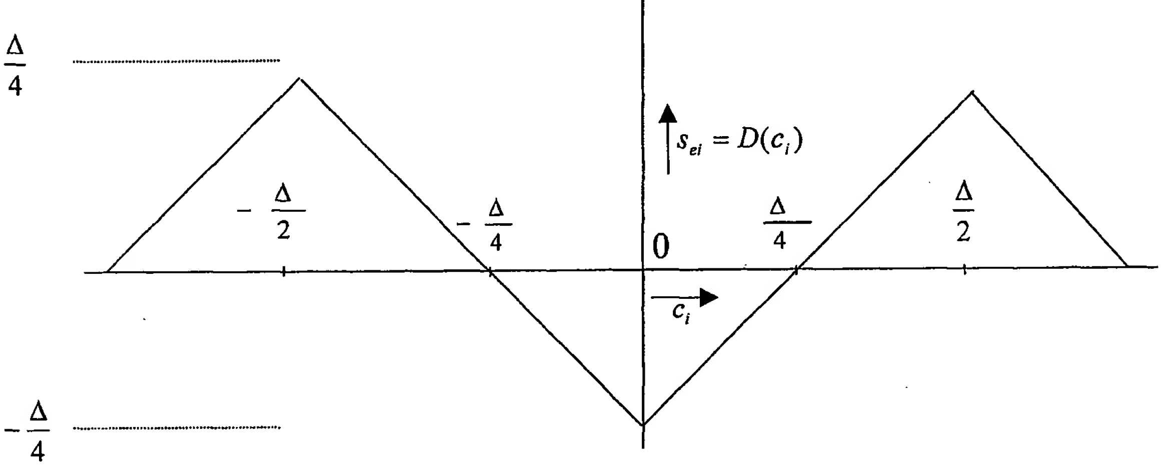
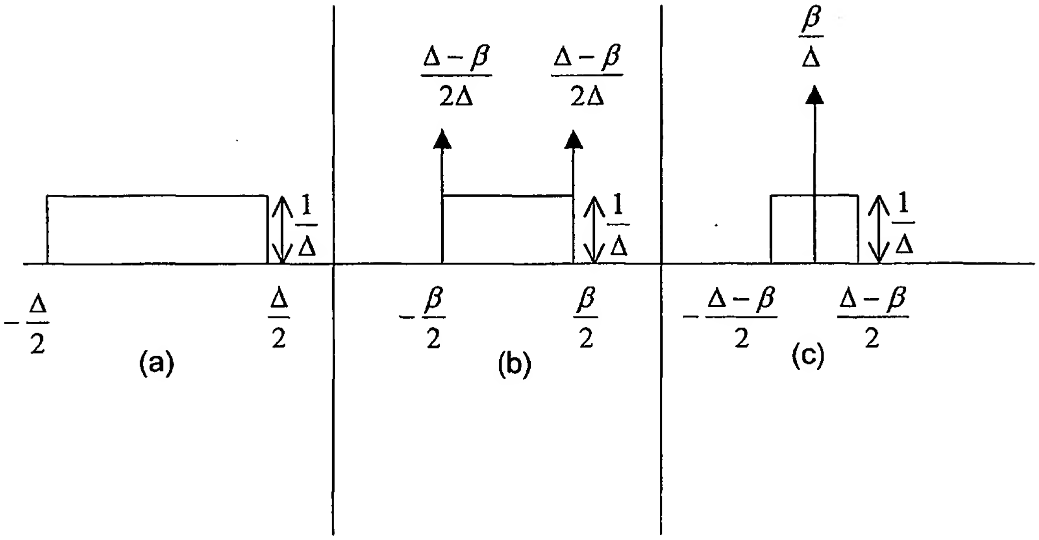


FIGURE 3


$\frac{1}{\Delta}$
$-\frac{\Delta}{2}$
$\frac{\Delta}{2}$
(a)
$\frac{\Delta-\beta}{2\Delta}$
$\frac{\Delta-\beta}{2\Delta}$
$\frac{1}{\Delta}$
$-\frac{\beta}{2}$
$\frac{\beta}{2}$
(b)
$\frac{\beta}{\Delta}$
$\frac{1}{\Delta}$
$-\frac{\Delta-\beta}{2}$
$\frac{\Delta-\beta}{2}$
(c)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/24468

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04K 1/02
US CL : 380/252, 253, 254
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/252, 253, 254

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Handbook of Applied Cryptography, Menezes, et. al. CRC Press1997

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

IEEE, Crypto Proceedings, West, EIC search, STN, Dialog

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,940,135 A (PETROVIC et. al.) 17 August 1999 Figure 3, Columns 2-6	1-13
Y	US 6175627 B1 (PETROVIC et. al.) 16 January 2001Columns 2--6	1-13
Y	US 3897591 A (LUNDSTROM et. al.) 29 July 1975	1-13
Y	US 3427399 A (EHRAT) 11 February 1969	1-13
Y	US 3133991 A (GUANELLA) 19 May 1964	1-13
Y	US 2836657 A (BARTELINK) 27 May 1958	1-13
Y	US 2426225 A (KRAUSE) 26 August 1947	1-13

□ Further documents are listed in the continuation of Box C. □ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search 26 SEPTEMBER 2001	Date of mailing of the international search report 09 JAN 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer Peggy Harrod GAIL HAYES Telephone No. (703) 308-4562